In the Claims:

Please note the following current set of claims:

1. (Previously presented) A method for providing cryptographic capabilities to a plurality of network users over a decentralized public network, the method comprising:

receiving a request for an access permission security profile on behalf of a network user that gives the network user the ability to access one or more objects associated with a domain according to the network user's membership in one or more groups within the domain;

authenticating the request from the network user according to an n-factor authentication suitable to the plurality of network users and verifying membership in the domain and the one or more groups;

creating the access permission security profile having an ephemeral crytpographic characterstic and derived from a combination of the user's membership in the one or more groups, wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object when one or more groups associated with the encrypted object match the network user's membership in one or more groups within the domain and to encrypt selected portions of a plaintext object to be accessed by other network user's when the other network user's membership in one or more groups within the domain also match the one or more groups associated with the selected portions of the plaintext object being encrypted; and

securely transmitting the access permission security profile to the network user over the network wherein the ephemeral cryptographic characteristic allows the network user in receipt of the

access permission security profile to perform cryptographic operations for a predetermined period of time.

2. (Previously presented) The method of claim 1, wherein the creating step comprises:

identifying one or more groups of network users who are to be provided with cryptographic capabilities according to each network user's membership in a particular combination of groups within the domain;

establishing one or more access codes for each group in the domain, wherein each access code is adapted to be combined with other components to form the cryptographic key; and

creating one or more access permission security profiles for each network user's membership in one or more different combination of groups in the domain, wherein the access permission security profile for each network user contains at least one access code in correspondence to the network user's membership in at least one group in the domain.

3. (Previously presented) The method of claim 1 , wherein each group is a category, organization, organizational unit, set of role based credentials, work project, geographical location, workgroup within the domain.

4. (Currently Amended) A method for providing decryption capabilities to a plurality of network users over a decentralized public network, the method comprising:

receiving a request for decryption capabilities on behalf of a network user that gives the network user the ability to decrypt one or more encrypted objects associated with a domain according to the network user's membership in one or more groups within the domain;

authenticating the request from the network user according to an n-factor authentication suitable to the plurality of network users and verifying membership in the domain and the one or more groups;

creating an access permission security profile derived from a combination of the user's membership in the one or more groups, wherein the combination of the user's membership in the one or more groups can be used to form a cryptographic key and decrypt selected portions of the one or more encrypted objects ;

receiving information associated with the selected portions of an encrypted object;

generating a cryptographic working key using the cryptographic key from the access permission security profile and the received information associated with the selected portions of the encrypted object; and

securely transmitting the cryptographic working key to the network user over the network allowing the network user to decrypt ~~other than~~ the selected portions of the encrypted object.

5. (Previously presented) The method of claim 4, wherein the creating step includes:

identifying one or more groups of network users who are to be provided with cryptographic capabilities according to each network user's membership in a particular combination of groups within the domain;

establishing one or more access codes for each group in the domain, wherein each access code is adapted to be combined with other components to form the cryptographic key; and

creating one or more access permission security profiles for each network user's membership in one or more different combination of groups in the domain, wherein the access permission

security profile for each network user contains at least one access code in correspondence to the network user's membership in at least one group in the domain.

6. (Previously presented) The method of claim 4 , wherein each group is a category, organization, organizational unit, set of role based credentials, work project, geographical location, workgroup within the domain.

7. (Previously presented) A method for cryptographically securing the distribution of information over a decentralized public network to a plurality of network users, the method comprising:

creating a computer representable data object including one or more embedded objects;

associating a pseudorandom cryptographic key with each of the one or more embedded objects of the data object to be encrypted;

encrypting each of the embedded objects using a working key derived from the respective pseudorandom cryptographic key associated with the embedded object and other components;

creating a set of one or more access permission credentials that identify the roles each of the plurality of network users may possess in a domain and their membership in one or more groups as defined by various combinations of the one or more access permission credentials;

assigning a member credential to each of the selected embedded objects, wherein the member credential is a specific combination of the one or more access permission credentials ensuring that only network users having a matching member credential are able to decrypt encrypted embedded objects of the data object;

inserting the pseudorandom cryptographic key in the header of each embedded object after first encrypting the pseudorandom cryptographic key with a credential key derived from the member credential associated with each embedded object;

transmitting the data object over the network having the encrypted pseudorandom key inserted in a portion of the embedded object; and

securely transmitting an access permission security profile, having an ephemeral crytpographic characterstic, to at least one network user from the plurality of network users wherein the access permission security profile for the at least one network user can be used to generate a credential key capable of decrypting the encrypted pseudorandom cryptographic key associated with the encrypted object because the member credential of the network user matches the member credentials associated with the encrypted object, wherein the ephemeral cryptographic characteristic allows the network user in receipt of the access permission security profile to perform cryptogrpahic operations for a predetermined period of time.

8. (Original) The method of claim 7, wherein the information is digital content.

9. (Currently amended) The method of claim 7, wherein securely transmitting further includes:

receiving a request for an access permission security profile on behalf of a network user; and

~~(ii)~~ authenticating the request from the network user using an n-factor authentication suitable to authenticate the plurality of network users.

10. (Previously presented) The method of claim 7, wherein securely transmitting further includes:

sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network;

receiving the request on behalf of the network user at the central server system; and

authenticating the request as from the network user using an n-factor authentication suitable to authenticate the plurality of network users.

11. (Previously presented) The method of claim 7, wherein the step of securely transmitting an access permission security profile is not performed if the user already has possession of an access permission security profile.

12. (Previously presented) The method of claim 7, wherein the working key may further be derived from at least a domain component, a maintenance component and, the pseudorandom cryptographic key.

13. (Currently amended) The method of claim 10 , wherein the access permission security profile is created by:

identifying one or more groups of network users who are to be provided with cryptographic capabilities;

establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and

creating one or more access permission security profiles for each network user's membership in one or more different combination of groups in the domain, wherein the access permission security profile for each network user contains at least one access code in correspondence to the network user's membership in at least one group in the domain.

14. (:Previously presented) The method of claim 13, wherein each group is a category, organization, organizational unit, set of role based credentials, work project, geographical location, workgroup within the domain.

15. (Original) The method of claim 1, 4 or 9, wherein the request is initiated in-band by the network user over the network.

16. (Original) The method of claim 1, 4, 9, 10, or 11, wherein the access permission security profile is in the form of a token that is adaptable to expire.

17. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of biometric identification.

18. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a hardware token.

19. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a software token.

20. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a user password.

21. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a record of time at which the request was made.

22. (Original) The method of claim 1, 4, 9, or 10, wherein the authenticating step includes the use of a record of the user's physical location.

23. (Cancelled)

24. (Cancelled)

25. (Cancelled)

26. (Cancelled)

27. (Cancelled)

28. (Cancelled)

29. (Cancelled)

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Cancelled)

34. (Cancelled)

35. (Cancelled)

36. (Cancelled)

37. (Cancelled)

38. (Cancelled)

39. (Cancelled)

40. (Cancelled)

41. (Cancelled)

42. (Cancelled)

43. (Cancelled)

44. (Cancelled)

45. (Cancelled)

46. (Cancelled).

47. (Cancelled).

48. (Cancelled)

49. (Cancelled)

50. (Cancelled)

51. (Cancelled)

52. (:Previously presented) A centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network, the system responsive to instructions executable on at least one processor associated with the system and further comprising:

a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network;

a set of server systems for managing the distribution of the member tokens;

means for requesting a member token from at least one server system;

a set of client systems, wherein each client system includes

means for receiving the requested member token, and

means for utilizing the cryptographic capabilities provided by said member token for selective encryption and decryption; and

means for securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network.

53. (Original) The system of claim 52, wherein each client system further includes user authentication means.

54. (Original) The system of claim 52, wherein the means for requesting a member token resides on each client system.

55. (Original) The system of claim 52, wherein means for authenticating a user resides on at least one server system.

56. (Original) The system of claim 52, wherein managing the distribution of the member tokens includes dynamic updating of the member tokens.

57. (Previously Amended) The method or system of claim 1, 4, 7 or 52, wherein the decentralized public network is the Internet.

58. (Previously Amended) The method or system of claim 1, 4, 7 or 52, wherein the decentralized public network is a cellular phone network.

59. (Original) The method of claim 1 wherein the access permission security profile received by the network user remains encrypted on a persistent memory device until decryption of one or more portions of the access permission security profile is deemed necessary to effectuate performing one or more cryptogrpahic operations on one or more objects.

60. (New) The method of claim 59 wherein the access permission security profile may be decrypted when the network user in receipt of the access permission security profile successfully performs an n-factor authentication operation.

61. (New) The method of claim 1 wherein the network user in receipt of the access permission secuirty profile can no longer perform cryptographic operations on one or more objects when the predetermined period of time associated with the ephemeral cryptographic characteristic has expired.

62. (New) The method of claim 1 wherein the network user in receipt of the access permission secuirty profile can not perform cryptographic operations on one or more objects when

one or more groups associated with the encrypted object do not match the network user's membership in one or more groups within the domain.

63. (Currently Amended) The method of claim 1 wherein decrypting selected portions of the encrypted object with the access permission security profile produces a secondary cryptographic key to be used in further decrypting ~~other than~~ the selected portions of the encrypted object.

64. (Original) The method of claim 1 wherein encrypting selected portions of the plaintext object includes encrypting a randomly generated value with respect to the one or more groups associated with plaintext object to be encrypted.

65. (Original) The method of claim 2 wherein the network user's membership in one or more different combination of groups corresponds to the network user's member credentials selected from a set of access permission credentials associated with the domain.

66. (Original) The method of claim 65 wherein encrypting selected portions of the plaintext object includes

encrypting the plaintext object using a randomly generated value;

generating a pseudorandom value by encrypting the randomly generated value in combination with one or more different credentials selected from the set of access permission credentials associated with the domain; and

embedding the pseudorandom value in the selected portions of the encrypted plaintext object.

67. (Canceled)

-